UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------x

UNITED STATES OF AMERICA	:	
-v.-	:	14 Cr. 404 (JMF)
BRENDAN JOHNSTON, a/k/a "BV1,"	:	
Defendant.	:	

----------x

GOVERNMENT'S SENTENCING MEMORANDUM

PREET BHARARA
United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

DANIEL S. NOBLE
Assistant United States Attorney
- Of Counsel -

U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

May 25, 2015

BY ECF & ELECTRONIC MAIL

The Honorable Jesse M. Furman
United States District Judge
Southern District of New York
Thurgood Marshall United States Courthouse
40 Centre Street
New York, New York 10007

Re: United States v. Brendan Johnston,
14 Cr. 404 (JMF)

Dear Judge Furman:

The Government respectfully submits this letter in advance of sentencing of Brendan Johnston (the "defendant") scheduled for Wednesday, May 27, 2015 at 3:30 p.m., and in response to the defendant's sentencing memorandum filed May 13, 2015 ("Def. Mem."). The United States Probation Office ("Probation Office") has calculated the applicable United States Sentencing Guidelines ("Guidelines" or "U.S.S.G.") range to be 46 to 57 months' imprisonment, as set forth in the Presentence Investigation Report dated May 1, 2015 (the "PSR"). The Government respectfully submits that a sentence within that Guidelines range is sufficient, but not greater than necessary, to provide just punishment, promote respect for the law, and provide adequate deterrence for a serious cybercrime offense.

BACKGROUND

A. The Blackshades Remote Access Tool ("RAT")

As set forth in detail in the PSR, between 2010 and 2014, an organization known as "Blackshades" sold malware to thousands of cybercriminals throughout the world. The leader of the Blackshades organization was Alex Yücel, a/k/a "Marjinz," a Swedish national. (PSR ¶ 28). Blackshades' flagship product was the Remote Access Tool, or "RAT," a sophisticated piece of malware that enabled cybercriminals remotely and surreptitiously to control other individuals' computers through the internet. (PSR ¶ 10). The Blackshades Organization sold the RAT for approximately $40 per license. (PSR ¶ 13). The RAT was marketed in online forums as a product that conveniently combined the features of several different types of hacking tools. For instance, one online advertisement read:

> Deciding between a RAT, a host booter, or controlling a botnet has never been easier.[1] With Blackshades . . . you get the best of all three – all in one with an easy to use, nice looking interface.
>
> Even better, Blackshades . . . does a lot of work for you – it can automatically map your ports, seed your torrent for you, and spread through AIM MSN, ICQ and USB devices. (PSR ¶ 13).

Once a user had purchased a license for the Blackshades RAT, the infection of victims' computers could be accomplished in a few ways, including tricking victims into clicking on a link contained in an email or hiring others to install the RAT on the victim's computer, which at times Blackshades itself offered to do for an additional fee. (PSR ¶ 14). The RAT also contained tools known as "spreaders" that helped users of the RAT infect victim computers by using computers that had already been infected further to spread the RAT. (PSR ¶ 15). Unlike legitimate remote access tools used by IT administrators, the Blackshades RAT did not require victims' consent prior to installation of the RAT, or notify victims when a remote session was active on their computers.

Upon infection of a victim's computer, the RAT user had free rein to, among other things: access, view, and steal the victim's documents, photographs, and other files; "hijack" the victim's files by requiring a ransom to "unlock" the files; employ the infected computer as a "bot" in a distributed denial of service ("DDoS") attack; record a victim's keystrokes through a "keylogger" to steal the victims' passwords and credit card numbers; and activate the victim's web camera to take still photographs or obtain a live feed of the victim without his or her knowledge. (PSR ¶¶ 20-24). All of these features could be controlled through the RAT's graphical interface, which allowed users easily to view and navigate all of the victim computers that they had infected. (PSR ¶ 18). Attached as Exhibit A are screenshots of the RAT user interface and certain RAT features, including the file hijacker, DDoS controller, and webcam controller.

In the course of its investigation of Blackshades, the Federal Bureau of Investigation ("FBI") seized and searched the Blackshades server, pursuant to a warrant. (PSR ¶ 32). A review of the records stored on the server revealed that there were more than 6,000 Blackshades customer accounts located in more than 100 countries. (PSR ¶ 33). Based on records obtained from various electronic payment processors, the Blackshades Organization earned at least $350,000 from sales of the RAT between September 2010 and April 2014. (PSR ¶ 30).

---

[1] A "host booter" is a tool that can be used to launch a denial of services ("DoS") attack, typically in the context of online video games. It disconnects or "boots" a person from a "host" (e.g., an online video game platform) and is typically done to cheat at the video game. A "botnet" typically refers to a network of infected computers or "bots." (PSR ¶ 13 n.2).

B. The Defendant's Role in the Blackshades Organization

Between the summer of 2011 through at least September 2012, the defendant, using the moniker "BV1," worked for Yücel as an administrator for Blackshades. In this role, the defendant's primarily responsibilities were helping market and sell the Blackshades Organization's products, including the RAT, and overseeing customer service representatives to provide troubleshooting and technical support for RAT users. (PSR ¶¶ 34-36, 39). Yücel paid the defendant a monthly fee of $500 and later permitted the defendant to keep the revenue generated through the sale of Blackshades' products, including the RAT, through certain types of electronic payment systems. (PSR ¶¶ 35, 38-39). During the time period that the defendant worked for the Blackshades Organization, the operation generated somewhere between $70,000 and $120,000 in sales. (PSR ¶ 44). The defendant, however, only earned approximately $6,500, assuming he made an average of $500 per month during the approximately 13 months that he worked for the Blackshades Organization.

The defendant initially met Yücel, the leader of the Blackshades Organization, on an online forum frequented by computer hackers called "HackForums.net," on which Blackshades was being marketed. (Def. Mem. 6). After the defendant began working for Yücel, he continued to market the Blackshades RAT and communicate with Blackshades users on HackForums. For example, on April 11, 2012, the defendant posted an advertisement that stated: "Blackshades is proud to present our newest product: Blackshades Stealth." The advertisement described the features of the product, including "screen capture," "webcam capture," "voice capture," and "keylogger." (PSR ¶ 36). As late as September 2012, the defendant continued to post messages marketing Blackshades on HackForums. For example, on September 25, 2012, the defendant posted a message that stated: "[W]e've just recently sold our 6,000th copy of our RAT" and that "we've just recently hit our 20,000th customer in total." (Id.).

In June 2012, the FBI arrested the co-creator of the Blackshades RAT, who used the moniker "Xviseral," in connection with another cybercrime investigation. (PSR ¶ 11 n.1). Xviseral began cooperating with the Government's investigation of Blackshades. Following Xviseral's arrest, the defendant quit working for the Blackshades Organization. The defendant subsequently wiped or disposed of the hard drives of the computers that the defendant had used in connection with Blackshades. (PSR ¶ 40).

C. Procedural History and Guidelines Calculation

On May 16, 2014, the defendant was arrested as part of the FBI's takedown of the Blackshades Organization and certain Blackshades customers.[2] The defendant was charged in a

[2] The co-creators of the Blackshades RAT, Alex Yücel and "Xviseral," have been arrested and have pled guilty to felony computer hacking charges; both await sentencing before Judge P. Kevin Castel. In addition, the FBI arrested three Blackshades customers in the New York/New

federal criminal complaint with conspiracy to commit computer hacking, in violation of 18 U.S.C. § 1030(b), and transmission of malware, in violation of 18 U.S.C. § 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(IV).

[redacted]

On November 21, 2014, the defendant pled guilty, pursuant to a plea agreement, to Count One of Information 14 Cr. 404 (JMF), which charged him with conspiracy to commit computer hacking, in violation of 18 U.S.C. § 1030(b). Pursuant to the plea agreement, the defendant agreed to forfeit all proceeds obtained from his work for the Blackshades Organization and any interest in the domain names used by Blackshades: www.blackshades.ru and www.bshades.eu. (PSR ¶ 6).

As calculated by the Probation Office, and as agreed by the parties in the plea agreement, the applicable Guidelines range is 46 to 57 months' imprisonment. (PSR ¶¶ 6, 104) The Probation Office recommends a term of imprisonment of 12 months and one day. (PSR at 26).

D. Victim Notification and Remediation

The Government took various steps during its investigation of the Blackshades Organization and after its takedown to attempt to identify and provide remediation to victims, including those individuals whose computers the defendant helped others to infect with the RAT. Unfortunately, for the reasons explained below, the FBI was unable to identify particular victims of the Blackshades Organization. (PSR ¶ 42).

Jersey area – Juan Sanchez, Kyle Fedorek, and Marlen Rappa – all of whom have pled guilty and been sentenced. Sanchez used the RAT primarily to spy on his girlfriend; Sanchez pled guilty to a misdemeanor computer hacking offense and was sentenced on December 23, 2014 by Magistrate Judge James C. Francis IV to one year of probation. Fedorek used the RAT primarily to steal victims' usernames and passwords for various financial, email, and social networking accounts; Fedorek pled guilty to a felony computer hacking offense and was sentenced on February 19, 2015 by Judge Vernon Broderick to a term imprisonment of two years. Rappa used the RAT primarily to steal photographs from victims' – mostly young women's – computers and spy on them using the RAT's webcam capture feature; Rappa pled guilty to a felony computer hacking offense and was sentenced on April 22, 2015 by Judge Valerie E. Caproni to a term of imprisonment of 12 months and one day.

During the investigation, the Government obtained court orders to install pen registers and trap-and-trace devices ("pen/trap devices") on certain Blackshades customers' Internet connections in order to identify the Internet protocol ("IP") addresses of computers that were communicating with the Blackshades customers' computers. By applying various filters to those IP addresses, the Government identified the IP addresses that were most likely to belong to victims. The Government then issued Grand Jury subpoenas to obtain subscriber information for those IP addresses in order to determine their physical locations. After identifying locations in the New York City area, FBI agents visited approximately ten different potential victims and attempted to obtain consent to search those computers for evidence of Blackshades infection. Unfortunately, none of the potential victims were willing to allow federal agents examine their computers. Thus, this house-to-house approach was not practicable.

In preparation for the takedown, which involved coordinated law enforcement actions in over a dozen countries, the Government applied for search warrants to seize electronic evidence from certain Blackshades customers' residences. A search of these computers revealed that victims' Blackshades-infected computers were identified on the RAT users' computer only by the name that the victim gave to his or her computer, such as "Jane's computer." Not surprisingly, none of the computer names contained the victims' full true name or other identifiers. The RAT also did not capture (or at least did not store) the IP addresses of the victims' computers, information that might otherwise have indicated at least the physical locations of the victims, such as whether they were in the United States or abroad.

At the time of the takedown, the Blackshades Organization had approximately 2,000 active customer accounts, each of which used a unique domain name to communicate with victims' computers (collectively, the "Customers' Domains"). In preparation for the takedown, and in a further effort to identify Blackshades victims, the Government applied for a court order to redirect all communications to the Customers' Domains to an FBI-controlled computer (the "FBI Computer"). The Government also applied for an Order authorizing the FBI to install a pen/trap device on the FBI Computer in order to capture the source IP addresses of computers that attempted to communicate with the Customers' Domains. However, an extremely large volume of IP addresses contacted the FBI Computer within the first hour, most of which were unlikely to have been IP addresses of victim computers. For example, IP addresses that contacted the FBI Computer included many that appeared to belong to so-called web crawlers, or computers that systematically browse the Internet, typically in order to index websites. Thus, identifying true victims from the huge number of IP addresses contacting the FBI Computer was also not practicable.

Notably, although the redirection of Customers' Domains and IP Addresses was unsuccessful in identifying victims, it did permanently disrupt the connection between victims' computers and Blackshades Customers' Domains. This effort, coupled with the seizure of the Blackshades Organization's server infrastructure, made it impossible for Blackshades customers, such as the defendant, to continue to access victims' computers.

Finally, the Government also took steps to educate the public about Blackshades and possible remedial action. For example, information about the Blackshades investigation and how to determine if a computer might be infected by Blackshades was posted on the FBI's website.[3] The Government also encouraged private industry to develop a Blackshades removal tool and publicize the existence of Blackshades on their websites.[4]

APPLICABLE LAW

The United States Sentencing Guidelines still provide strong guidance to the Court following United States v. Booker, 543 U.S. 220 (2005), and United States v. Crosby, 397 F.3d 103 (2d Cir. 2005). Although Booker held that the Guidelines are no longer mandatory, it also held that the Guidelines remain in place and that district courts must "consult" the Guidelines and "take them into account" when sentencing. Booker, 543 U.S. at 264. As the Supreme Court stated, "a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range" — that "should be the starting point and the initial benchmark." Gall v. United States, 552 U.S. 38, 49 (2007).

After that calculation, however, a sentencing judge must consider seven factors outlined in 18 U.S.C. § 3553(a): "the nature and circumstances of the offense and the history and characteristics of the defendant," 18 U.S.C. § 3553(a)(1); the four legitimate purposes of sentencing, see id. § 3553(a)(2); "the kinds of sentences available," id. § 3553(a)(3); the Guidelines range itself, see id. § 3553(a)(4); any relevant policy statement by the Sentencing Commission, see id. § 3553(a)(5); "the need to avoid unwarranted sentence disparities among defendants," id. § 3553(a)(6); and "the need to provide restitution to any victims," id. § 3553(a)(7). See Gall, 552 U.S. at 50 & n.6.

In determining the appropriate sentence, Section 3553(a) directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;

(B) to afford adequate deterrence to criminal conduct;

---

[3] See, e.g., http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown; http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/could-your-computer-be-infected-by-blackshades.

[4] See, e.g., http://www.symantec.com/connect/blogs/blackshades-coordinated-takedown-leads-multiple-arrests

(C) to protect the public from further crimes of the defendant; and

(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

DISCUSSION

Application of the Section 3553(a) factors to the facts of this case supports a sentence within the advisory Guidelines range. Because of the serious nature of the defendant's cyber offense, the long period of time in which the defendant was involved with the Blackshades Organization, and the need to deter others from distributing harmful malware like the Blackshades RAT, the Government submits that a sentence within the advisory Guidelines range of 46 to 57 months' imprisonment is appropriate.

A sentence within the applicable Guidelines range is warranted to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment. See 18 U.S.C. § 3553(a)(2)(A). The seriousness of the defendant's criminal conduct requires little elaboration. Over the course of approximately 13 months, the defendant helped Yücel market and sell the Blackshades RAT, including on HackForums, and oversaw a team of customer support personnel who provided technical assistance to RAT users. In doing so, the defendant directly enabled hundreds, if not thousands, of RAT users to infect and effectively take complete control of victims' computers without their knowledge or consent. Although the FBI did not obtain any evidence that the defendant himself used the RAT to infect computers (the defendant wiped the hard drives of the computers he used in connection with Blackshades), his actions nevertheless helped other RAT users to do so.

The substantial harm caused by the defendant's actions is demonstrated by the cases of two Blackshades customers who were prosecuted in this District: Kyle Fedorek and Marlen Rappa. Fedorek used the Blackshades RAT to infect over 400 victims' computers, from which he obtained approximately 90 unauthorized access devices in the form of financial account user credentials. Rappa used the Blackshades RAT to infect almost 100 victims' computers, from which he downloaded thousands of personal photographs, videos, and other files. Rappa also used the Blackshades webcam feature to spy on his victims and take still screenshots of them, including when they were naked and having sex. Fedorek's and Rappa's egregious invasions of their victims' privacy and theft of their victims' financial and personal information illustrates the types of harms that flowed directly from the defendant's distribution of the Blackshades RAT.

In his sentencing memorandum, the defendant claims that he initially believed that Blackshades was a "legitimate company" (Def. Mem. 7) and that he continued to market and

sell the Blackshades RAT for only "about 45 days" after he realized the "illicit" nature of the RAT (Def. Mem. 9-10). There is substantial reason to doubt the defendant's claim, which calls into quesiton whether he has fully accepted responsibility for his crime.[5] First and foremost, the illicit nature of the Blackshades RAT is immediately apparent from its own features, including the "DDoS" controller, "file hijacker," and "spreader" tools. Thus, standard anti-virus programs frequently included Blackshades in their lists of malware to block. In addition, unlike legitimate remote access tools, victims were not asked for their consent before the RAT was installed on their computers, nor were victims notified when the RAT was running on their computers. It is also telling that the Blackshades RAT was advertised on HackForums, a site regularly frequented by computer hackers, and was marketed as an "all-in-one" computer hacking tool comprising a remote access controller, booter, and DDoS controller.

[redacted][6]

Based on the defendant's own use of the RAT, and given that he was charged with marketing the RAT (including on HackForums) and overseeing the personnel who provided technical assistance to RAT customers, it is clear that the defendant was in a position to understand the illicit nature of the RAT and its potential to cause substantial damage to victims' computers from early on in his tenure with the Blackshades Organization.

In addition to the seriousness of the offense, a Guidelines sentence is also necessary to achieve adequate general deterrence. See 18 U.S.C. § 3553(a)(2)(B). Computer hacking is becoming an ever more prevalent threat in society. Using inexpensive and easy-to-use hacking tools such as the Blackshades RAT (which only cost $40 to purchase), cyber criminals can obtain access to and control over others' computers through the internet. With such unfettered access, cybercriminals can steal the victims' personal and financial information,

---

[5] Also troubling is the explanation that the defendant provided to the Probation Office for his extensive marijuana use. (PSR ¶¶ 87-89). The defendant asserted that he was given a prescription for medical marijuana to treat [redacted] migraine headaches, but could not provide the name of the doctor who prescribed the marijuana. It is difficult to understand how marijuana, a depressant, could legitimately be prescribed to treat [redacted] headaches.

[6] [redacted]

spy on them, or enlist their computers to commit additional cybercrimes, such as DDoS attacks. Further, given the anonymity of the Internet and the proliferation of tools available to cyber criminals to evade law enforcement, significant penalties are necessary to send a message that the illegal distribution of malware will not go unpunished.

The defendant argues that sentencing him to a term of imprisonment in order to deter others from committing similar crimes is "narrow-sighted" and "ignores his unique background, circumstances, and culpability." (Def. Mem. 18). While the Court can and should consider the defendant's history and characteristics, including his lack of criminal history and [redacted] these factors simply do not support the drastic downward variance that the defendant seeks. In requesting a term of probation, the defendant places much emphasis on his history of [redacted] (See Def. Mem. 2-8, 11-14). Although this is certainly a mitigating factor, it cannot bear the weight that the defendant places on it. As an initial matter, the defendant's offense conduct cannot be attributed to his [redacted] Nevertheless, the defendant argues that [redacted] contributed to his decision to work for the Blackshades Organization and to distribute the RAT because it, in effect, gave him a sense of purpose and positive feedback. While this may be true, it cannot fully explain, much less undermine the need adequately to punish, the defendant's decision to help sell and support others' use of dangerous malware.

In addition, the fact that the defendant suffered from [redacted] is, unfortunately, not unique among the individuals who have been prosecuted for their involvement with Blackshades. Indeed, all three of the Blackshades customers who were prosecuted and have been sentenced in this District suffered from serious mental health issues at the time that they were using Blackshades and sought leniency on that basis. As such, the defendant's [redacted] is not so unique as to undermine the need for a sentence that promotes general deterrence. Furthermore, the two Blackshades customers whose conduct was most egregious – Fedorek and Rappa – were sentenced to terms of imprisonment of two years and a year and a day, respectively. Although there is no evidence that the defendant himself used the RAT to hack into victims' computers and steal their financial and personal information, his actions in marketing, selling, and providing technical support directly enabled other RAT users to do so. Thus, a sentence that includes a term of incarceration is also necessary to avoid unwarranted sentencing disparities among defendants. See 18 U.S.C. § 3553(a)(6).

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court impose a sentence within the advisory Guidelines range of 46 to 57 months' imprisonment. In addition, at sentencing the Government will submit a proposed Forfeiture Order for the Court's consideration seeking forfeiture of $6,500, which represents the approximate amount of proceeds that the defendant earned from his work for the Blackshades Organization, and any interest of the defendant in the domain names used by the Blackshades Organization.

Respectfully submitted,

PREET BHARARA
United States Attorney

By: 
Daniel S. Noble
Assistant United States Attorney
(212) 637-2239

cc: Michael Zweiback, Esq. (by electronic mail)